INVESTMENT BUSINESS GUIDE TO THE PREVENTION OF MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING

APPROVED BY THE BOARD OF COMMISSIONERS - 27/8/24
ISSUED BY FINANCIAL SERVICES COMMISSION – 3 September 2024
PUBLISHED - 3 September 2024
COMMENCEMENT DATE - 3 September 2024

Contents

1. Introduction

1.1 The Financial Services Commission (the "FSC") is the regulatory body with prudential and AML/CFT/CPF oversight of Investment Business Services Providers ("IBSPs"). As a sector, Investment Business has been subject to regulation in the Virgin Islands since 1996. Since that time, the Virgin Islands has expanded the scope of regulatory oversight to address evolving practices for mutual funds, investment managers, fund administrators and other businesses that operate within the securities sector. The Virgin Islands has been at the forefront of the development of regulatory standards and the production of typology reports that relate to IBSPs.

1.2 The regulatory regime for investment business is mainly captured by primary legislation – the Securities and Investment Business Act, 2010 (SIBA). The investment business sector captures several regulated products, such as investment funds, as well as the provision of several areas of services that can be provided in the sector:

- Investment Manager,
- Fund Administrator,
- Investment Advisor,
- Custodial Services,
- Administrator

1.3 The regime allows for registration, authorisation and licensing based on the scope of business to be conducted. In some cases, a licence can be provided for multiple services, which can impact risks being faced by an IBSP.

1.4 As a sector, IBSPs are challenged with many risks, including risks that are inherent to the nature of products and services provided, as well as external risks that they may face. These risks include bad actors who may seek to use an investment product or other service to further nefarious activities, as well as for money laundering ("ML), terrorist financing ("TF") and proliferation financing ("PF").

1.5 These Guidelines have been developed for the benefit of IBSPs and persons who may seek to become licensed as an IBSP under SIBA. These Guidelines also buttress the provisions for compliance with the Anti-Money Laundering and Terrorist Financing Code of Practice (the "AMLTFCOP") including the Explanatory Notes[1], the Anti-Money Laundering Regulations ("AML Regulations"), the Regulatory Code (the "RC") and the Financial Services Commission Act (the "FSC Act"). They highlight the risks IBSPs may face, including sanctions evasion, illicit financing activities and other financial crimes. Additionally, these Guidelines are geared towards assisting IBSPs in the implementation of a risk-based approach when applying measures to mitigate against ML, TF and PF risks.

1.6 To aid persons in understanding and identifying ML, TF and PF risks the Financial Action Task Force (FATF) developed its *FATF Typology Reports – Money Laundering and Terrorist Financing in the Securities Sector*.[2] In addition, the publication of the FATF Guidance for a Risk-Based Approach for the Securities

[1] Explanatory Notes provide guidance on implementing the requirements of the AMTFCOP and AML Regulations. The FSC will take implementation and compliance with the Explanatory Notes into account when assessing compliance by a regulated entity including an IBSP.

[2] The FATF Typology Report can be found at here.

Sector published in October 2018 has provided additional clarity of the unique risks impacting IBSPs. Therefore, these documents have been factored into the development of these Guidelines. All IBSPs are guided to keep up to date with these and future publications from the FATF that may be relevant to the sector.

1.7 Comprehensive AML/CFT/CPF compliance by IBSPs, and other regulated entities operating in or from within the Virgin Islands ("VI") is essential to remain up-to-date with evolving risks and threats that could adversely impact operations and compliance. This Guide also serves as a complement to the ongoing need to report and engage with the FSC and other Competent Authorities, including law enforcement agencies to achieve optimal results in preventing ML, TF and PF risks from being realized. These agencies include the Office of the Governor, Attorney General's Chambers, Royal Virgin Islands Police Force (RVIPF), the BVI Financial Investigation Agency (FIA) and the BVI International Tax Authority (ITA).

2. Applicable Persons to Whom these Guidelines Apply

2.1. These Guidelines are relevant for all persons who are licensed to provide management, administration, custodial or other services in relation to investment business activities or other securities or investment business products operating in or from within the VI. Any entity wishing to provide one of these services in or from within the Virgin Islands is required to be licensed by the FSC. IBSPs may be licensed to operate under the following categories:

- Dealing in Investments as an Agent
- Dealing in Investments as a Principal
- Arranging deals in investment
- Managing Segregated Portfolios (Excluding Mutual Funds)
- Managing Mutual Funds
- Managing Pension Schemes
- Managing Insurance Products
- Managing Other Types of Business
- Providing Investment Advice (Excluding Mutual Funds)
- Providing Investment Advice for Mutual Funds
- Custody of Investments (Excluding Mutual Funds)
- Custody of Investments for Mutual Funds
- Administration of Investment (Excluding Mutual Funds)
- Administration of Investments for Mutual Funds
- Operating as an Investment Exchange

The scope of each category of business for which an IBSP may be licensed can be found at the Appendix to these Guidelines.

Scope of Applicable Business

2.2. The scope of investment business that can be conducted is vast. As a well-developed industry, providing services in the investment business sector falls broadly into a number of functions, or combination of functions.

2.3. The Investment business sector in the VI primarily includes three general categories:

- Asset managers (including advisers), investment managers (including advisers) and custodians;
- Securities Brokers/Dealers; and
- Asset and investment administrators

Brokers and Dealers

2.4. Brokers or dealers in securities are the most active participants in the investment business sector in the VI. A broker typically acts as an agent for an investor and enters the securities markets on behalf of an investor to buy or sell a security. In this buying and selling process, some dealers provide liquidity to the capital market by its own capacity of buying and selling. A specific vulnerability associated with broker-dealers is their reliance on another financial institution's CDD process. A broker-dealer might assume that, because another reporting entity has opened an account for a customer, the customer does not pose ML/TF/PF risks for them. If illicit assets are successfully placed at a depository institution, the broker-dealer may assume that, because the funds are from an institution which is subject to AML/CFT rules, the Customer does not pose a ML/TF/PF risk and therefore will accept cheques from that institution to fund a securities account. Once a securities account is funded, a customer can engage in a number of transactions that further conceal the source of his or her illicit funds, thereby successfully layering and integrating illicit assets that were placed through a depository institution. Importantly, it is the responsibility of each institution to ensure that the proper CDD process has been completed.

2.5. Brokers and dealers in securities can be distinguished from those securities intermediaries that are regulated as asset managers, custodians and portfolio managers. The role of a broker and a dealer are clearly delineated from those of custodians and managers. In fact, different registration and regulatory standards may apply to them. Nonetheless, functions can be housed in the same entity by means of multiple registrations. Such advisory functions and broker-dealer functions may be conducted under the same registration.

Asset Managers, Administrators and Custodians

2.6. The role of the asset manager, custodian and portfolio manager is generally to advise on the composition of an investment portfolio or to hold securities of local or foreign customers or to manage the contents of investment accounts for retail or institutional Customers respectively. Portfolio management typically involves the provision of financial services in a managed relationship with Customers who are often of high net worth. The value and complexity of products offered to high-net-worth customers, together with the international nature of the business, make the provision of wealth management services potentially attractive to money launderers, to disguise their illicit assets. The custodian services, regardless of the nationality of an investor, have the same potential to be a money launderer as portfolio management and asset management services.

2.7. Additionally, the typical operations of service providers in and around the investment business sector will see large transactions and currency flows into and out of products. Investments being placed

with an IBSP may come from multiple countries. Frequent and large cross-border flows of transactions present their own risks. In aggregate, these factors make investment business an attractive target for persons seeking to misuse these vehicles for criminal purposes.

2.8. The securities products can be utilised in the layering and integration stages of money laundering once illicit assets are placed in the financial system. However, the investment business sector is relatively inhospitable to the placement of illicit assets into the financial system. Nevertheless, certain securities products do pose identifiable ML/TF/PF vulnerabilities even at the placement stage. For example, illicit proceeds may directly be placed for buying securities.
The complexity of the investment business sector and the variety of intermediary roles involved highlight that no one-size-fits-all AML/CFT approach should be applied. However, this variety and complexity highlights the importance of IBSPs understanding of how their business arrangements raise ML/TF/PF risks both directly (e.g., through transactions executed by customers) and indirectly (e.g., risks associated with the underlying customers of the securities provider's customers, or risks associated with the possibility that an intermediary or other entity on which the securities provider relies to perform a task fails to do so).

3. Objective

3.1. These Guidelines give clarity to specific AML/CFT/CPF obligations for IBSPs under VI law, which includes requirements for robust customer due diligence and enhanced customer due diligence procedures, transaction monitoring, proper recordkeeping measures, amongst other requirements. Further, these Guidelines give context to the development of compliance and risk frameworks necessary to fulfill statutory reporting obligations and monitoring and assessment of risks that are present in the management and administration of mutual funds, investment management, securities trading, the provision of custodial services, and other activities of IBSPs that fall under the remit of SIBA. Based on the complexity of securities business, as well as the multiple roles that a service provider may play, it is important to recognise that there may be a need to revisit risks and risk mitigation strategies on a more frequent basis.

4. ML/TF/PF Risks and IBSPs

4.1. In light of the many risk-based factors elevating risks present in the conduct of securities business, it is important for IBSPs to understand the importance of mitigating against the risks of ML, TF, PF and other illicit activities. AML/CFT/CPF requirements for entities operating in or from within the Virgin Islands are primarily set out in the following legislation:

- the AMLTFCOP;
- AML Regulations;
- Proceeds of Criminal Conduct Act ("PCCA");
- Criminal Justice (International Cooperation) Act, 1993;
- Counter-Terrorism Act, 2021 ("CTA"), Proliferation Financing (Prohibition) Act, 2021 ("PFPA"); and

- the relevant Orders-in-Council related to terrorism, terrorist financing and proliferation financing.

4.2. The Virgin Islands Money Laundering Risk Assessment 2022, Virgin Islands Financial Services Sector Terrorist Financing Risk Assessment 2020 and the Virgin Islands Proliferation Financing Risk Assessment 2022 identify various ML/TF/PF threats and vulnerabilities that IBSPs are exposed to and these risks must be accounted for within the IBSP's procedures, policies and controls. IBSPs are also alerted to risks by Competent Authorities on an ongoing basis. In addition, the general public are also alerted to scams and frauds detected by Competent Authorities that occur predominantly in relation to securities business.

4.3. IBSPs are required to appoint a Compliance Officer, unless otherwise exempt. However, such an exemption is not an exemption from the requirement to undertake the compliance functions. The duties of the Compliance Officer include, among other things, the development and implementation of the compliance framework which addresses all areas of operation. Importantly, the compliance function rests with the Board of Directors and to ensure compliance measures are effective, the Board should ensure it remains apprised of ongoing compliance efforts. The compliance framework must therefore be designed to prevent risks of an IBSP being used for ML, TF, PF and other risks. The Board and Senior Management of an IBSP should, therefore, ensure that periodic quality assurance reviews are conducted to assess the adequacy of AML/CFT/CPF procedures and other controls.

4.4. Compliance frameworks must also be sufficiently comprehensive to detect internal risks, where employees may become complicit parties in assisting bad actors with ML, TF, PF or other criminal activities. Importantly, IBSPs must be vigilant to ensure their compliance framework can detect where securities are being used to generate illicit assets. Further, FATF Recommendations 10, 11 and 17 in relation to customer due diligence, recordkeeping and reliance on third parties, respectively, are especially important for IBSPs to ensure that proper customer due diligence information is collected and maintained for all customers, intermediaries and relevant third parties upon whom a reliance is being placed (collectively referred to as 'due diligence subjects'). It is important for IBSPs to also ensure that they identify the beneficial owners of relevant due diligence subjects. In the conduct of due diligence, it is also critical for IBSPs to carry out thorough checks to also identify and verify controllers of relevant due diligence subjects. IBSPs must also consider other FATF Recommendations, and in particular, Recommendations 12, 19, 20, 21, 24 and 25 in the development of their compliance framework

4.5. IBSPs are gatekeepers to the securities sector. In such an important role, it is critical that IBSPs ensure that the securities sector within which they operate retains its integrity of the markets and broader global economic systems. Financial crimes such as insider trading or market manipulation or other predicate offences to money laundering can occur in securities markets. Therefore, an IBSP's risk mitigation strategy must keep pace with the fast-evolving threats within the sector given the complexity and size of transactions that can exacerbate risks. IBSPs must also be vigilant for other predicate offences occurring within structures, such as corruption and tax evasion. This vigilance must also be extended to individual customers who may be conducting illegal activities or have committed offences. To be effective in assessing potential risks, it is also important for IBSPs to examine the beneficial ownership and control of structures that include securities products or services including all legal persons and arrangements.

4.6. Awareness of the risks that exist with the formation of securities products, or in the provision of services for investments into securities or other assets is critical for IBSPs to develop a resilient compliance framework. IBSPs should ensure that they identify and assess indicators of ML, TF and PF risks that they may be exposed to, which may be informed by "a range of factors[3], including:

a) The nature, diversity and complexity of its business, products and target markets;
b) The proportion of customers identified as high risk;
c) The jurisdictions in which the securities provider is operating or otherwise exposed to, either through its own activities or the activities of customers, especially jurisdictions with greater vulnerability due to contextual and other risk factors such as the prevalence of crime, corruption, or financing of terrorism, the general level and quality of the jurisdiction's prosecutorial and law enforcement efforts relating to AML/CFT, the regulatory and supervisory regime and controls and transparency of beneficial ownership;
d) The distribution channels through which the securities provider distributes its products, including the extent to wish the securities provider deals directly with the customer and the extent to which it relies (or is allowed to rely) on third parties to conduct CDD or other AML/CFT obligations, the complexity of the transaction change, the use of technology and the extent to which intermediation networks are used;
e) The internal and external (such as audits carried out by independent third parties, where applicable) control functions and regulatory findings; and
f) The expected volume and size of its transactions, considering the usual activity of the securities provider and the profile of its customers.

4.7. There is helpful guidance issued by international standard setters that will assist IBSPs with applying a risk-based approach. For example, the FATF published its *Risk-Based Approach Guidance for the Securities Sector* in October 2018, which provided key elements for applying a risk-based approach (RBA) to AML/CFT/CPF as it relates to IBSPs, among other things[4].

4.8. The following publications are also relevant to IBSPs:

- FATF Report – Money Laundering and Terrorist Financing in the Securities Sector.
- IOSCO – Anti-Money Laundering Guidance on Collective Investment Schemes.
- Virgin Islands Financial Services Sector Terrorist Financing Risk Assessment Report, 2020.
- Virgin Islands Proliferation Financing Risk Assessment, 2022.
- Virgin Islands Money Laundering Risk Assessment, 2022.

4.9. Taken together, these documents provide guidance to IBSPs on indicators that may point to an investment product being used for nefarious purposes, whether to generate or further ML, TF, PF or other illicit activity. Incorporating these guidance documents into an IBSP's systems and controls will help timely identification of potential suspicious activities and mitigate risk.

[3] The list of factors has been cited from the FATF Guidance for a Risk-Based Approach for the Securities Sector, 2018.
[4] This Guidance was issued with the proviso that it be read in conjunction with the FATF Recommendations, and in particular, Recommendations 1, 10, 13, 17, 19, 20 and 26 and their Interpretive Notes (INR), as well as other Guidance documents issued by FATF.

4.10. Given the global nature of the securities sector, IBSPs must consider cross-border threats of ML, TF and PF on an ongoing basis. Cross-Border threats, vulnerabilities and risk may emanate from many scenarios, including: -

a) High volumes of cross border transactions that may obscure the movement of monies and other assets connected to the proceeds of crime that may be integrated into the financial system through an IBSP to launder such proceeds, or otherwise being used to finance terrorism or proliferation activities.
b) Political and/or economic instability in countries where an IBSP may have exposure (i.e. though investments, investors/clients or third-party service providers) that has an elevated risk of bribery and corruption, and where corrupt practices are frequently engaged in as a means to conduct business.
c) Tax evasion conducted through an IBSP where a client may seek to circumvent tax authorities to unlawfully evade paying taxes owed to a Tax Authority.
d) Exposure to a sanctioned person through a client or third party that uses the IBSP to evade sanctions and/or embargoes.

5. Risks to be Monitored by IBSPs

5.1 IBSPs have a wide range of risk factors that could impact their AML/CFT/CPF compliance framework. The risks that they are exposed to may arise from their engagement with customers, intermediaries and Third Parties. Risks are assessed based on country/geographic risk factors, product risk, service risk, risks associated with delivery channels and customer risk. In reviewing potential risks, and the probability of those risks, IBSPs must consider the nature of their business, as well as the use of intermediaries and/or Third Parties in the execution of transactions.

Customer Risk

5.2 IBSPs may be exposed to ML/TF/PF and other risks through their operations where criminals may seek to obscure the origin and ownership of criminally obtained assets through placement in legal structures or legal arrangements. The following are examples of customer risk:

- a customer places illicit proceeds into an investment vehicle as a result of poor customer due diligence procedures being in place, resulting in the IBSP being used to launder monies.
- when bad actors use corporate structures such as a business company as a front to give the appearance of being a legitimate business, and subsequently seeks investment services to funnel assets to support terrorist activities, further proliferation financing activities or other financial crimes.
- a customer of an IBSP may seek to place increasingly specific investments that may be as a result of that customer having knowledge not known to the market and attempts to engage in insider trading which is a predicate offence to ML.

5.3 Insider trading and market manipulation can undermine the integrity of financial markets. These crimes, together with ML and TF risks in relation to trading of securities by brokers, and other investment

business professionals being used by bad actors include the obfuscation of key details of the date of operations, origin of assets and beneficial ownership information. As such, IBSPs must ensure that they are aware of the material risks presented by persons who may be engaged in insider trading, market manipulation or other illegal activities. Examples of red flags that could be indicative of market manipulation include:

- Securities or funds transfers between parties without an apparent relationship.
- Securities transactions occur across many jurisdictions, and in particular high-risk jurisdictions.
- Two or more unrelated accounts at the brokerage house trade an illiquid or low-priced security/asset suddenly and simultaneously.
- Transactions between the same or related parties structured solely so that one side incurs a loss while the other incurs a gain.
- The customer deposits a large number of physical securities at the brokerage house.
- The physical securities are titled differently to the name on the account.
- The company at issue has no apparent business, revenues or products.
- The company at issue has experienced frequent or continuous changes in its business structure and/or undergoes frequent material changes in business strategy or its line of business.
- The low priced, illiquid, or low volume security/asset at issue has failed to make required regulatory disclosures/ history of regulatory violations.
- A customer engages in prearranged or other non-competitive securities trading, including wash or cross trades of illiquid or low-priced securities.
- The customer deposits physical securities together with a request to journal the shares into multiple accounts that do not appear to be related, or to sell or otherwise transfer ownership of the shares.
- A customer's transactions include a pattern of receiving physical securities or receiving incoming shares transfers that are sold with the proceeds wire transferred out of the account.

5.4 Examples of red flags that could be indicative of insider trading:

- The customer makes a large purchase or sale of a security/asset, or option on a security/asset, shortly before news is issued that affects the price of the security/asset.
- The customer is known to have friends or family who work for the securities issuer or related parities to the transaction.
- A customer's trading patterns suggest that he or she may have inside information.
- The customer's purchase does not correspond to his or her investment profile. For example, the customer may never have invested in equity securities, but does so at an opportune time.
- A customer trades in selective security/asset just after opening the account and makes sizeable profit in each trade.
- A customer trading in small amount of shares suddenly takes a sizable position in a specific security/asset and makes a considerable profit on it.
- A Customer earns a sizable profit by generating a considerable portion of market volume in illiquid security/asset.

Service/Product/Transaction Risk

5.5 Risks may also be presented where clients seek services that are unusual or unconventional. For example, IBSPs may be sought out by proliferation financiers to invest in companies that manufacture or refine materials that are dual-use goods that have the potential to be used in nuclear armaments or other WMD. These investments may be leveraged towards the diversion of the dual-use goods to be used for nefarious activities. Complex transactions may also be an avenue used by bad actors who are seeking to launder money as a means to obscure the proceeds of crime. Additionally, bad actors may also seek to execute more frequent transactions to make tracing proceeds of crime more difficult.

Geographic Risk

5.6 IBSPs whose business model includes exposure to jurisdictions that lack an effective framework for the supervision of AML/CFT/CPF risks should ensure that thorough risk assessments are always undertaken. IBSPs risk assessment frameworks must have regard to higher risk jurisdictions for AML/CFT as identified by international standards setters such as FATF. All IBSPs are expected to conduct Geographic/Country Risk[5] assessments as a component of their overall Institutional Risk Assessment Framework. In all cases, IBSPs must also carry out checks to corroborate source of funds and sources of wealth in their AML/CFT/CPF evaluations. IBSPs should also carry out their independent due diligence and verifications in all cases, which should be informed by the level of risk exposure.

Risk Monitoring and Mitigation

5.7 Ongoing monitoring conducted by IBSPs must be sufficiently robust to detect anomalous transaction patterns, including spikes in activity, unusual volumes and values of transactions, development of new and unexplained relationships and networks[6] between clients and other parties or any other unusual and suspicious behaviour. Where such suspicious activity is detected, including where a client withdraws from entering into a business relationship based on a reluctance or refusal to provide information sought in relation to due diligence, an IBSP should examine the circumstances behind these actions and consider the need to file a suspicious transaction/activity report (STR/SAR).

5.8 Risk mitigation strategies that are targeted to specific areas of business, whether by service, product, client type, geographic location or a combination of these attributes should also be developed with an aim to improve granularity of the risk indicators that could indicate ML, TF, PF or other criminal activities. It is important for IBSPs to carry out risk assessments on the nature of the products and/or services they offer toward developing strong risk mitigation strategies. Therefore, it is important to determine the level of risk associated with each product and service being offered by an IBSP. Additionally, IBSPs should also assess risks associated with differing client types. The inherent risks associated with institutional investors differ from those associated with retail investors. Risks associated with geographic locations (also referred to as Country Risk) must also be assessed, as there may be

[5] Geographic/Country Risk should include assessment of the AML/CFT/CPF framework that exists in a subject country, as well as the level of political stability, current and forecasted economic stability and other data that are relevant to assessing corruption, sanctions compliance and other factors.

[6] Unexplained relationships and networks may be integrated into an existing client relationship with an aim of obscuring transactions, thereby making it difficult to monitor and trace the movement of funds. The use of unexplained networks can also add increased difficulty in identifying suspicious patterns. Ensuring that an IBSP has effective screening can aid in detecting these unexplained networks.

heightened risks of corrupt practices, terrorist activities or other crimes that could increase exposures to ML, TF and PF risks. IBSPs should ensure that their internal controls are developed in accordance with section 11(3) of the AMLTFCOP[7].

5.9 IBSPs must remain vigilant to emerging risks and new typologies that may diminish existing risk mitigation strategies. As the strategies of bad actors evolve, IBSPs must be diligent in ensuring that their risk assessment frameworks are regularly updated and calibrated to changes in risks.

5.10 IBSPs must also guard against the erosion of their compliance culture from external factors. These may include pressures from affiliated entities within a Group of Companies, or other institutions to reduce or dilute compliance provisions. Further, IBSPs must ensure that reliance is not placed on due diligence or other compliance measures undertaken by other entities that are not in line with FATF Recommendation 17, as well as sections 31, 31A and 31B of the AMLTFCOP. IBSPs are, therefore, required to maintain robust compliance provisions that appropriately address ML, TF, PF risks or risks of financial crime on an ongoing basis.

6. Institutional Risk Assessments

6.1 IBSPs are required to assess the risk inherent in their business, taking into consideration relevant factors, i.e. their customers, countries or geographical areas to which they are exposed, the products, services or transactions they offer, and the delivery channels used to access customers. An institutional risk assessment should assist an entity or a professional to holistically understand the ML/TF/PF risks to which it or he or she is exposed and identify the areas that should be proritised to combat ML/TF/PF. Firm-specific Institutional Risk Assessments must ensure that the ML, TF and PF risks being faced by an IBSP are factored into the development of its Risk Assessment Framework. For an IBSP, particular attention must also be paid to its technology and cyber security risk it faces.

6.2 An important part of the risk assessment is to identify the level of risk posed by each relevant factor and develop a risk rating. IBSPs must ensure that risk identification is carried out in relation to all products, services, customers, delivery channels and new technologies. Risk identification must also be carried out for geographic risks and risks that may be present as well as risks introduced by the engagement of third parties. Examples are provided in **Table 1** below as a guide but are not exhaustive. Any risk assessment must account for specific risk faced by individual IBSPs.

Table 1 – Examples of Risks Criteria re IBSPs

Area of Risk	Description	Example of Potential Risks

[7] Explanatory Note (i) following section 11 of the AMLTFCOP states that, "*The risk-based approach essentially enables an entity and a professional to balance the risks associated with their business, including customers, products, services, transactions, delivery channels and geographic connections to the established measures to contain and properly deal with those risks. It provides an element of flexibility that enables an entity or a professional to devise and apply its or his or her own systems of internal controls and management to deal with specific cases and circumstances to forestall and prevent acts of money laundering, terrorist financing and proliferation financing in relation to the entity or professional. It is considered to be a more effective approach.*

Customer	This requires an overall assessment of the risks posed by customers and requires an entity or a professional to consider the risk profiles of its customer base and determine the extent to which the entity's or professional's customer base consists of higher risk customers. This overall assessment is based on the individual customer risk assessments that must be conducted in accordance with section 12(1)(b) of this Code. [8]	A customer may be connected to a high-risk jurisdiction through the location of their business activities, through residency or other means. A customer may be a Politically Exposed Person by way of elected office or other high-level governmental or military appointment.
Geographic/Country	This examines the extent to which an entity or professional's business is exposed to ML/TF/PF risks based on the countries with which it interacts, whether directly or via customers. The aim is to understand the level of interaction an entity or professional has with countries that pose a higher risk of ML/TF. An entity or professional is considered to interact with a country, where: • it operates or engages in business, in, from within or with a country, including the Virgin Islands; • it has customers (including beneficial owners) that are based, operate, or have personal or business links in the country; • its customers receive funds from or transmit funds to the country; and • its customers' funds were generated for use in the business relationship or one-off transaction in the country. In assessing the ML/TF/PF risks of the countries to which it is exposed, an entity and a professional should give due consideration to: • the effectiveness of the country's regime as identified by credible sources, such as the FATF, CFATF, IMF, GIFCS, etc.; • whether the country is either considered or identified as a high risk country (including a country identified as having higher risk by the FATF or CFATF); • whether the country is subject to sanctions, embargos or similar measures	Investment strategies may expose an IBSP to a country with political instability or existing sanctions (where licenses can be obtained to invest in specified areas) that present elevated levels of risk. An IBSP may be exposed to geographic risks where a significant portion of the client base and/or the nature of the investment activities are located in a jurisdiction with poor AML/CFT/CPF compliance, heightened risks in relation to corruption, drug trafficking or other illicit financing activities.

[8] See Explanatory Note (iii) to Section 12 of AMLTFCOP.

	issued (e.g., sanctions imposed by the UNSC or the UK); • whether the country or geographic area has been identified by reliable and credible sources (such as the FATF, CFATF, IMF, GIFCS, etc.) as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within the country; • whether the country or geographic area has been identified by reliable and credible sources (such as the FATF, CFATF, IMF, GIFCS, etc.) as having high levels of corruption; and • the level of criminal conduct related to ML/TF within the country.[9]	
Product / Service/Transaction	This is an assessment of the extent to which the products, services and/or transactions offered can be exploited for ML/TF/PF purposes. Entities and professionals should consider: • the nature, scale and diversity of its business' products and services; • the complexity of each of the products and services offered; • whether products and services include new technologies; • the volume and size of its transactions (as it relates to each type of transaction available); • whether the characteristics of products, services and transactions facilitate anonymity of customers, layers of opacity, or can readily transcend international borders (this latter category would include online banking facilities, stored value cards, international wire transfers, private investment companies and trusts); • the extent to which a product, service or transaction may be susceptible to an unknown third party to conduct business via another person; • the extent to which certain transactions involve multiple persons and jurisdictions; • the extent to which third party payments can be accepted; and	Investments in high-risk assets such as rare earth minerals may elevate the risks inherent with a service or a product which an IBSP may be facilitating.

[9] See Explanatory Note (iii) to Section 12 of AMLTFCOP.

	• whether transactions are more cash-based.[10]	
Delivery Channel	This relates to the manner in which products and services are offered to a customer and an assessment of the extent that these mediums can be exploited by customers or other third parties for ML/TF/PF purposes. The assessment should consider the extent to which the entity or professional: • receives customers on a face-to-face basis; • receives customers on a non-face to face basis, for example: ▪ via telephone or online interaction; ▪ via an agent or intermediary; ▪ via introduction from a third party; or ▪ via digital or electronic means. For assessing the risks associated with non-face to face business, the entity or professional should consider: • Where establishing relationships over telephone or email interaction: ▪ the possibility that an applicant for business or customer may be able to impersonate another person; and ▪ the extent to which an applicant for business or customer may provide falsified documentation in support of his or her application; • Where using agents, intermediaries or introductions from third parties: ▪ the country in which the agents, intermediaries or third parties are incorporated or operate and the level of ML/TF risks posed by that country; ▪ whether the agents, intermediaries or third parties are subject to some form of AML/CFT oversight; ▪ whether a third party making introductions maintains relevant CDD information and documentation in accordance with the terms of the third party agreements and as required pursuant to sections 31 to 31B of this Code; and	An IBSP's engagement with clients may be facilitated through intermediaries and online platforms dedicated to onboarding clients, which may expose the IBSP to elevated risks where the intermediaries and platforms have inadequate ML, TF and PF controls.

[10] See Explanatory Note (iii) to Section 12 of AMLTFCOP.

	▪ whether agents or intermediaries are monitored to ensure adequate CDD measures are being undertaken when attracting clients; and • In the case of use of digital or electronic means for the establishment of a business relationship or conduct of transactions: ▪ the extent to which the use of digital or electronic means exposes the entity or professional to cyber-attacks and security breaches and the consequent possibility of stolen data and identity fraud; ▪ whether the entity or professional has measures in place to adequately and appropriately protect itself or him or her from cyberattacks and security breaches posed by use of the digital or electronic means; and ▪ whether there are unknown vulnerabilities due to the novelty of the digital or electronic means being utilised. [11]	
Third Party Risk	The ML/TF risks emanating from other third-parties with which an entity engages; for instance service providers, product suppliers, affiliates, contractors, consultants and advisors, etc.[12]	Third Parties engaged to facilitate trades of securities and other assets may expose an IBSP to ML, TF or PF risks where the Third Party does not adequately mitigate risks within its operations.

6.3 When conducting institutional risk assessments IBSPs should also review the FATF Recommendations and Methodology, the various Risk Assessment Reports of the Virgin Islands and this Guidance together with all relevant laws and regulations. The Boards of Directors should also develop and adopt a Risk Tolerance Statement towards the development of IBSPs' institutional risk assessment frameworks.

6.4 IBSPs should address their risk management strategies to ensure that they are sufficiently robust to mitigate ML, TF and PF risks. Testing of risk management strategies should be conducted on an incremental basis to build resilience of the entire risk management framework. Further, IBSPs should carefully record issues that occur that could have a bearing on risk assessments as these should cause the risk assessment to be reassessed. These may include: (i) internal suspicious transactions; (ii) compliance

[11] See Explanatory Note (iii) to Section 12 of AMLTFCOP.
[12] Ibid

failures; (iii) intelligence from internal staff; (iv) findings from the internal audit function; (v) findings from supervisory reviews, (vi) new risk assessments issued at the national level, (e) corporate reorganizations, entering new markets or new business lines.

7. Matters for Consideration

7.1 Understanding Beneficial Ownership and Control

7.1.1 The fundamental part of the AML/CFT regime in the VI is for relevant persons such as IBSPs to understand is the need to identify, verify and keep up date information on the beneficial owners of an applicant for business, customer or one-off transaction.

7.1.2 A Beneficial Owner is a natural person who ultimately owns or controls an applicant for business or a customer, on whose behalf a transaction or activity is being conducted.13 Control includes any natural person who has influence over the activities of an applicant for business or customer (with or without any ownership interests). This makes it clear that the provisions related to identification and verification of beneficial owners extend beyond legal ownership, or what is simply recorded in the register of members but goes to ultimate ownership.

7.1.3 The beneficial owner of a legal person including a company or partnership is an individual person who:

- holds, directly or indirectly, more than 10% of the shares in the entity;
- holds, directly or indirectly, more than 10% of the voting rights in the entity;
- holds the right, directly or indirectly, to appoint or remove a majority of the board of directors of the entity or in case of a partnership remove eh general partner(s); and
- has the right to exercise, or actually exercises, significant influence or control over the entity.

7.1.4 The beneficial owner is a trustee of a trust is

- the trustees of that trust (in their capacity as such) hold, directly or indirectly, more than 10% of the shares in the entity;
- the trustees of that trust (in their capacity as such) hold, directly or indirectly, more than 10% of the voting rights in the entity;
- the trustees of that trust (in their capacity as such) hold the right, directly or indirectly, to appoint or remove a majority of the board of directors of the company;

[13] See section 2(1) of the AMLTFCOP.

- the trustees of that trust (in their capacity as such) have the right to exercise, or actually exercise, significant influence or control over the company;
- any natural person, characteristic or class of persons entitled to a vested right in the trust; and
- the Trustee, Settlor, Protector, or any other identified person who has control over the trust and ability to take certain actions and make decisions.

7.1.5 When identifying and verifying the beneficial owners, regard must be had for nominee arrangements where the listed shareholder may be acting on behalf of another individual (i.e. the beneficial owner). IBSP must always inquire into whether nominee arrangements exist in relation to applicants for business, customers, clients and individual one-off transactions.

7.1.6 The following sections provide IBSPs with information on undertaking measures (i.e. CDD and KYC) which would be appropriate for identifying and verifying beneficial owners.

7.2 Customer Due Diligence

7.2.1 In onboarding new customers, IBSPs should exercise care in ensuring that comprehensive due diligence and risk assessments are carried out on customers – both individuals and institutional clients. To ensure that due diligence measures are sufficiently robust to determine the true beneficial owners and controllers. These measures should also include verification procedures to ensure that individuals or legal structures are not used to obfuscate the true beneficial owners and/or controllers through the use of 'strawmen' or nominee arrangements or other means. Due diligence and risk assessments should also be performed for one-off transactions. If at any time during the relationship with a customer where the IBSP has any doubts about the veracity of information collected in relation to a customer, the IBSP must carry out further due diligence assessments. Where information does not provide clarity on the bona fides of the customer and there is suspicion of monies being sourced from proceeds of crime, the IBSP should terminate the relationship and file a suspicious transaction report with the BVI Financial Investigation Agency.

7.2.2 Part III of the AMLTFCOP provides the detailed requirements for undertaking customer due diligence ("CDD"). IBSPs are considered to have business relationships with persons who seek services or products in the course of providing investment business services. In such circumstances, IBSPs are required to carry out CDD to identify and verify the applicant for business or customer. Similar identity verification is required in the case of one-off transactions.

7.2.3 In addition to carrying out CDD measures when one sets up a business relationship with a customer or carries out an occasional transaction, CDD should also be carried out if the IBSP:

- suspects ML, TF or PF;
- has determined that the relationship presents a higher-than-normal risk; and
- has any doubt about any information provided by the customer for identification or verification purposes.

7.2.4 To effectively carry out the act of CDD, a IBSP must:

- have systems to identify those persons who cannot produce standard documents;
- take account of the greater potential for money laundering in higher risk cases, specifically in respect of politically exposed persons[14];
- not deal with persons or entities if due diligence cannot be executed, or the results are not satisfactory; or
- have a system for keeping customer information up-to-date.

7.3 Applying CDD Measures

7.3.1 The extent to which CDD measures are applied may vary to the extent permitted or required by law, based on the ML/TF/PF risk identified or associated with the business relationship or one-off transaction. This means that the amount or type of information obtained, or the extent to which this information is verified, must be increased where the risk associated with the business relationship or transaction is higher. It may also be simplified where the risk associated with the business relationship or transaction is lower. It should, however, be noted that applying and adopting simplified CDD measures is not acceptable where there is a suspicion of ML or TF or PF, or where specific higher-risk scenarios apply.

7.3.2 IBSPs should be aware of risk factors and ML/TF/PF warning signs in order to develop strong risk mitigation measures and controls to satisfactorily assess the ML/FT/PF risks pertaining to a particular business relationship or transaction. Schedule 3 of the AMLFTCOP provides guidance on risk factors and red flags which may impact transactions in the investment business sector. These may include:

a) Criminal convictions of persons connected to the ownership of the asset;
b) Assets involved in the securitization are difficult to quantify or are in locations difficult to access;
c) Assets exhibit opaqueness and/or inconsistencies with respect to ownership;
d) Assets which appear overvalued or whose characteristics are not in keeping with the sector and known risk within that sector and/or asset class;
e) Customer/investor is more concerned about the subscription and distribution terms of the product when compared to other information related to the investment;
f) Sudden and unexplained subscriptions and transfers request;
g) Requests to pay distributions to a third party with little connection or unrelated to the owner; and
h) A customer or investor that exhibits unusual concern with compliance with AML/CFT/CPF reporting requirements or other AML/CFT/CPF policies and procedures.

7.3.3 IBSPs should note that the AMLTFCOP allows relevant entities to utilise technological mechanisms to effect CDD and record keeping. Therefore, IBSPs must be able to demonstrate to the FSC that any

[14] Politically exposed persons (PEPs) are persons (foreign and domestic) who are, or have been, entrusted with prominent public functions (Heads of state or government, politicians, senior government officials, judicial or military officials, senior executives of statutory bodies, senior political party officials) or who hold prominent functions within an international organization (senior managers and members of the Board).

technological means are consistent with the requirements to undertake CDD and primarily with respect to identifying and verifying applicants for business and customers, including beneficial owners and controllers. Any technological development must not hinder the exchange of information with the FSC, other competent authorities and law enforcement agencies.

7.4 Simplified CDD Measures

7.4.1 Where a IBSP determines that a customer poses a significantly low risk and having regard to the AMLTFCOP, the ML, TF an PF risks identified by a Virgin Islands' national risk assessment, or a risk assessment conducted by a competent authority, law enforcement agency or any other authority with responsibility relating to ML, TF or PF in the Virgin Islands, simplified CDD measures may be applied. In cases where an IBSP determines that simplified CDD measures may be applied, the following actions may be taken:

a) fewer elements of customer identification data may be obtained (e.g. production of one form of ID instead of two);
b) simplified identity verification procedures may be employed;
c) collection of specific information or the carrying out of specific measures to understand the purpose and intended nature of the business relationship may not be required (the purpose and nature of the business relationship may be inferred from the type of transactions or business relationship established);
d) the identity of the customer and the beneficial owner(s) may be verified after the establishment of the business relationship;
e) in the case of an existing business relationship, the frequency of customer identification updates may be reduced; and
f) the degree and extent of on-going monitoring and scrutiny of transactions may be reduced, based on a reasonable monetary threshold.

7.5 Enhanced CDD Measures (ECDD)

7.5.1 ECDD refers to the additional steps an entity is required to undertake to limit or manage the risk posed by a customer who poses a higher level of risk. This will be the case in relation, for instance, to a politically exposed person, a person from a jurisdiction that is considered to pose a high ML/TF/PF risk or a person who trades in products that are of a complex nature. In cases where an IBSP determines that ECDD measures may be applied, the following actions may be taken:

a) additional identifying information from a wider variety of, or more robust sources should be obtained and corroborated and the information used to inform the individual customer's risk profile;
b) additional searches (e.g. verifiable adverse internet searches) should be carried out to better inform the individual customer's risk profile;
c) where appropriate, further verification procedures should be undertaken on the customer or beneficial owner to better understand the risk that the customer or beneficial owner may pose to the IBSP;
d) the source of funds and wealth involved in the transaction or business relationship should be verified to satisfy the IBSP that they do not constitute the proceeds of crime;
e) the information provided with regard to the destination of funds and the reasons for the transaction should be evaluated; and
f) additional information about the purpose and intended nature of the transaction or the business relationship should be sought and verified.

7.5.2 IBSPs should also consider the following specific higher-risk factors, which may also trigger the need to conduct ECDD:

a) Clients are connected to industries or sectors where opportunities for ML, TF and PF are particularly prevalent. These may include clients that:
    i. become a politically exposed person;
    ii. operate or reside in a jurisdiction that is subject to recent sanctions or have been recently listed as having major deficiencies in their AML/CFT/CPF framework; and
    iii. is discovered to have exposure to persons or subjects evidenced as participating in corrupt practices.
b) The client:
    i. is involved in the shipment and/or sale of dual purpose goods;
    ii. has been transferred to a IBSP's portfolio with little or no notification;
    iii. changes or expands their business activities into volatile markets;
    iv. frequently requests endorsements from the IBSP on their bona fides; and
    v. refuses to send complete information following a request made for more clarification for a transaction or other activity.

7.5.3 The FATF Guidance for a Risk-Based Approach for the Securities Sector provides details that relevant IBSPs should, amongst other factors, consider in carrying out risk identification and assessment.

An extract of these factors has been provided in Box 1 below. IBSPs should likewise pay particular attention to the Interpretive Notes to FATF Recommendation 10 relating to customer due diligence.

Box 1. Non Exhaustive List of Examples of Enhanced Due Diligence/Simplified Due Diligence measures (see also INR.10)

Enhanced Due Diligence

- Obtaining additional customer information, such as the customer's reputation and background from a wider variety of sources before the establishment of the business relationship and using the information to inform the customer risk profile
- Carrying out additional searches (e.g. internet searches using independent and open sources) to better inform the customer risk profile
- Carrying out additional searches focused on financial crime risk indicator (i.e. negative news screening) to better assess the customer risk profile
- Obtaining additional or more particular information about the intermediary's underlying customer base and its AML/CFT controls
- Undertaking further verification procedures on the customer or beneficial owner to better understand the risk that the customer or beneficial owner may be involved in criminal activity
- Obtaining additional information about the customer's source of wealth or the source of funds involved in the transaction
- Verifying the source of funds or wealth involved in the transaction or business relationship to seek to ensure they do not constitute the proceeds of crime
- Evaluating the information provided with regard to the destination of funds and the reasons for the transaction
- Seeking and verifying additional information from the customer about the purpose and intended nature of the transaction or the business relationship
- Requiring that the redemption payment is made through the initial account used for investment or an account in the sole or joint name of the customer
- Increasing the frequency and intensity of transaction monitoring

Simplified Due Diligence

- Limiting the extent, type or timing of CDD measures
- Obtaining fewer pieces of customer identification data
- Altering the type of verification carried out on customer's identity
- Inferring the purpose and nature of the transactions or business relationship established based on the type of transaction carried out or the relationship established, without collecting additional information or carrying out additional measures related to understanding the nature and purpose
- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if transaction or account values rise above a defined monetary threshold)
- Reducing the frequency of customer identification updates if the securities provider implements or is required to implement a periodic review process based on a formal cycle
- Reducing the degree and extent of on-going monitoring and scrutiny of transactions, for example based on a reasonable monetary threshold

7.5.4 Where an IBSP is unable to verify the identity of an individual, it should not enter a business relationship or execute a one-off transaction with that individual except as provided for under the section 23 of the AMLTCOP and the related explanatory notes, including where the transaction is time sensitive and the AML/CFT/CPF risk is adequately mitigated. If the business relationship already exists, the IBSP should terminate the business relationship. In all circumstances the IBSP should consider filing a suspicious transaction report with the FIA, in relation to the customer or individual.

7.6 Ongoing CDD

7.6.1 Once a business relationship is established, IBSPs have an obligation to ensure that CDD/ECDD measures are carried out on an ongoing basis. Such measures are required to determine whether executed transactions are consistent with IBSP's information about the customer and the nature and purpose of the business relationship, wherever appropriate. These ongoing CDD/ECDD measures should allow IBSPs to identify changes in customer profiles (for example, their behaviour, use of products and the amount of money involved), and to keep them up to date, which may require the application of enhanced CDD measures. Ongoing CDD/ECDD monitoring and updating of information held should be carried out with sufficient frequency that has been informed by a documented risk-based approach. Importantly, an IBSP should ensure that its compliance framework integrates the ability to update CDD/ECDD information immediately based on a triggering event that results in material changes to a client's profile or circumstances. An example of a triggering event can include an existing client becoming a PEP by way of an election or appointment to a post that would qualify them as a PEP, which results in a change in their risk profile and risk score.

7.7 Transaction Monitoring

7.7.1 An essential component in identifying transactions that are potentially suspicious is transaction monitoring. Transactions that do not fit the behaviour expected from a customer's profile, or that deviate from the usual pattern of transactions, may be potentially suspicious. IBSPs must also consider non-cash transactions in their monitoring processes; for example, a non-cash transaction includes requests for the provision of corporate documents. Where new patterns of transactions emerge, IBSPs should ensure that measures are taken to determine whether there is an increased risk of ML, TF or PF, as well as to document changes in pattern and the assessment of ML/TF/PF risks. Monitoring should, therefore, be carried out on an ongoing basis.

7.7.2 IBSPs should ensure that they have systems that allow for thorough transaction monitoring. This may be achieved by a combination of strategies; examples include the use of screening tools as well as the implementation of threshold alerts that identify transactions that exceed expected amounts. Using technological solutions that allow for scenarios gleaned from FATF Typology reports to be added to transaction monitoring systems can also strengthen the overall AML/CFT/CPF systems of an IBSP. IBSPs may also apply 'Negative News Screening' to aid in their transaction monitoring efforts.

7.7.3 Transaction monitoring systems may be manual or automated based on the volume of transactions processed by an IBSP on a regular basis. However, where automated systems are used, IBSPs

should understand their system tolerances ~~operating rules~~, verify their suitability and integrity on a regular basis and verify that they take account of identified ML/TF/PF risks.

7.7.4 The level of transaction monitoring should be based on IBSP's institutional risk assessment and individual customer risk profiles, with enhanced monitoring being executed in higher risk situations. The adequacy of an IBSP's monitoring system, and the criteria used to determine the level of monitoring to be implemented, should be reviewed regularly to ensure that they are in line with the IBSP's AML/CFT/CPF risk programme.

7.7.5 Transactions performed or initiated by an outsourced party must also be subject to regular monitoring under the same conditions as transactions with the IBSP itself. Such monitoring should be conducted under the IBSP's control by the IBSP itself, or in collaboration with the third party, based on appropriate agreements complying with the requirements of the AMLTFCOP.

7.7.6 IBSPs should consider creating thresholds in relation to clients' assets under management, based on a risk-based approach, to determine the level of scrutiny for transaction monitoring purposes. Additionally, IBSPs should properly document, retain and communicate with the relevant personnel including senior management and front-line staff, the results of their monitoring, as well as any queries raised and resolved. IBSPs must also undertake relevant training.

7.8 Recordkeeping

7.8.1 Section 13 of the Act and Part IV of the AMLTFCOP require IBSPs to maintain records that are sufficient to show and explain transactions and fiscal positions, as well as ensure that all customer due diligence records are obtained and maintained. Records to be maintained include[15]:

- the records required by the Anti-money Laundering Regulations and the AMLTFCOP for purposes of establishing customer due diligence, undertaking risk assessments, compliance auditing, law enforcement, facilitating the strengthening of the entity's or professional's systems of internal control and facilitating responses to requests for information pursuant to the provisions of the regulations, the AMLTFCOP or any other enactment or for regulatory or investigative purposes;
- the policies and procedures of the entity or professional regarding relevant internal control measures;
- the internal suspicious activity reports made and the supporting documentation;
- the decisions of the Reporting Officer in relation to suspicious activity reports and the basis for the decisions;
- the activities relating to complex or unusual large or unusual patterns of transactions undertaken or transactions which do not demonstrate any apparent economic or visible lawful purpose or, in relation to a customer, are unusual having regard to the customer's pattern of previous business or known sources of business;
- the activities of customers and transactions that are connected with jurisdictions which do not or insufficiently apply the FATF Recommendations;
- the activities of customers and transactions which relate to jurisdictions on which sanctions, embargos or other restrictions are imposed; *and*
- the account files and business correspondence with respect to transactions and customers.

[15] See section 45 of AMLTFCOP.

7.8.2 IBSPs must also ensure that records are maintained in a manner that allows for retrieval without undue delay as set out by regulation 11 of the AML Regulations.

7.8.3 Part I, Divisions 3 of the RC also sets out requirements that are essential for IBSPs, which includes recordkeeping. The RC requires IBSPs to maintain records that enable the FSC to monitor compliance with its regulatory and AML/CFT/PF obligations.

7.9 Reliance on Third Parties

7.9.1 The extent of reliance on or dealing through third parties or intermediaries will impact the ML, TF and PF risks that an IBSP may be exposed to. Where an IBSP relies on a third party to undertake any portion of the process to identify and verify beneficial owners and controllers connected to assets being managed or administered, due care should be taken to assess their, and by extension the third party's AML/CFT/CPF policies and procedures to ensure that they are sufficiently developed and effective to detect and mitigate ML, TF and PF risks

7.9.2 Section 31 of the AMLTFCOP sets out requirements wherein regulated entities can rely on an introduction made for an applicant for business. Sections 31A and 31B of the AMLTFCOP also require IBSPs to enter into written agreements and test relationships with third parties. Regulations 7, 7A and 7B of the AML Regulations also set out requirements for IBSPs in relation to reliance on Introducers. These requirements are in line with FATF Recommendation 17 and reflect good business practices for risk mitigation against ML, TF, PF and other financial crimes where an IBSP may rely on a third-party introduction.

7.9.3 A risk assessment taken in relation to introducers is required and should assist an IBSP to holistically understand the ML/TF/PF risks to which it or he or she is exposed and identify the areas that should be prioritised to combat ML/TF/PF. Where an introducer is assessed as being high risk, an IBSP should determine whether the risks identified could be properly and consistently mitigated. If the elevated risks cannot be mitigated, an IBSP should not enter into a relationship with the high-risk introducer. Alternatively, where an introducer is assessed as having a lower risk (that is, medium risk or low risk), an IBSP should ensure that it establishes agreements in accordance with section 31A of the AMLTFCOP, as well as monitor the relationship to ensure that changes in risk exposures are detected. In all cases, the IBSP should ensure that relationships with introducers are subject to testing and monitoring in accordance with sections 31, 31A and 31B of the AMLTFCOP.

7.9.4 IBSPs should give particular attention to the risks based on the business activities/profession of the Third Party, as well as geographic and service risks that may be presented. These risks can be elevated where a country has a higher prevalence of bribery, corruption and poor AML/CFT/CPF systems, the latter of which could be evidenced by an FATF Mutual Evaluation Report.

7.9.5 An important part of the risk assessment is to identify the level of risks posed by each relevant factor and develop a risk rating. IBSPs must be able to identify the areas that pose higher risks and apply enhanced measures accordingly. External factors can influence the frequency and/or risk rating of a Third Party. External factors may include whether: a) the Third Party is subject to AML/CFT/CPF supervision; b) the Third Party is an affiliate of a group of companies that include the IBSP; or c) the Third Party has been subject to censure or penalties from law enforcement agencies or self-regulatory bodies. Therefore, IBSPs

that rely on Third Parties may have to undertake more frequent risk assessments based on changing business activities, geopolitical factors or other circumstances that could impact a Third Party with whom they have a relationship. Records of a IBSP's risk assessment of Third Parties must be maintained and made available to the FSC and all other competent authorities. Such records will include the findings, recommendations and steps taken to implement any recommendations. It is expected that the personnel at the highest level of an IBSP (i.e. directors/senior management) will consider and execute the findings of risk assessments conducted in relation to Third Parties.

7.9.6 Where an IBSP develops a suspicion of ML, TF or PF in relation to a Third Party, a suspicious activity report should be filed with the FIA. The IBSP should also take all appropriate steps to discontinue its relationship with the Third Party. Where a IBSP exits its relationship with a Third Party, the IBSP must undertake thorough risk assessments of all related business prior to entering into direct business relationships with the affected clients.

8. Terrorist Financing

8.1 A "terrorist act" is defined by the FATF as any act constituting an offence under a range of widely adopted international conventions"[16]. The FATF further defines terrorist financing as the financing of terrorist acts, and of terrorists and terrorist organisations. These definitions are aligned with those specified in the Counter-Terrorism Act, 2021 and relevant Orders-in-Council (OIC) that criminalise terrorism and terrorist financing within the VI. As with ML, a jurisdiction's TF risk is considered to be a function of its TF threats and vulnerabilities. A threat in the TF context, being a person or group of people, object or activity with the potential to cause harm to the state, society, economy etc., through the raising, moving, storing or using of funds and other assets.

8.2 Terrorist Financing is criminalized in the VI through:

a) **Counter-Terrorism Act, 2021** - makes provision for the detection, prevention, prosecution and conviction of terrorist and terrorist financing activities and gives effect to international conventions and resolutions for the countering of terrorism and terrorist financing including UNSCRs 1267 and 1373. It implements travel bans and requirements to report suspicious activities and provides for the detention and confiscation of goods suspected to be terrorist property.
b) **Anti-terrorism (Financial and Other Measures) (Overseas Territories) Order, 2002** - restricts transactions in terrorist property and creates extra-territorial jurisdiction in respect of offences relative to terrorism such as engaging in fundraising or money laundering, using or possessing property or arranging fundraising activities, for terrorist purposes. It also enables the registration and enforcement of foreign confiscation orders by an order of the Governor and provides measures for the enforcement of forfeiture orders in relation to money or other property which is likely to be used for the purposes of terrorism; proceeds of the commission of acts of terrorism; and proceeds of acts carried out for the purposes of terrorism.
c) **The Counter-Terrorism (Sanctions) (Overseas Territories) Order 2020 and the Counter-Terrorism (International Sanctions) (Overseas Territories) Order 2020 -** these Orders extend the

[16] Pg 125, International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, The FATF Recommendations, June 2019.

Counter-Terrorism (Sanctions) (EU Exit) Regulations 2019 and Counter-Terrorism (International Sanctions) (EU Exit) Regulations 2019 respectively to the Virgin Islands and allow for the designation of persons involved in terrorism related activities, freezing and unfreezing of assets and the issuing of licences in respect of otherwise prohibited activities. They also allow the sharing of information to enable the effective implementation and enforcement of the UK sanctions regime.

8.3 In addition, the **Afghanistan (Sanctions) (Overseas Territories) Order, 2020** and the **ISIL (Da'esh) and Al-Qaida (United Nations Sanctions) (Overseas Territories) Order, 2020** give effect to the UNSCRs which impose targeted financial sanctions against Afghanistan, Al-Qaida and ISIL (Da'esh). They enable relevant authorities to take the necessary action to freeze funds of designated persons and entities in respect of targeted individuals, groups, undertakings and entities associated with the Taliban, ISIL and Al-Qaida, and prohibit funds being made available to such persons.

8.4 Effectively combatting terrorism and terrorist financing relies on the efforts of a wide cross-section of businesses, professionals and Competent Authorities. The threat of TF has been assessed as having a lower risk within the VI; however, risks do exist. To ensure that IBSPs are taking appropriate measures to detect and prevent TF, compliance systems must be designed in a manner that allows for the identification and disruption of financial flows to terrorists, terrorist organisations, financiers and sympathisers. IBSPs, should ensure that their systems and controls are properly developed to aid in identifying the terrorist financing risks and vulnerabilities to which they are exposed and also in the development of their systems and controls to prevent, detect and report terrorist financing.

8.5 IBSPs should be aware that the complex nature of products offered within the investment business sector can make them attractive to a subset of higher-risk customers. While the investment business sector has not been identified as being particularly vulnerable to TF based on typology reports and other guidance issued by the international community, IBSPs should remain vigilant to potential vulnerabilities and threats that products and services may be used or exposed to TF activities. Guidance for IBSPs on red flags and activities which may raise suspicion for TF are found in the AMLTFCOP and further elaborated in section 11 of this Guideline. IBSPs should note the similarities between red flags for ML and TF but ensure they are able to identify the differences in order to take the appropriate action.

9. Proliferation Financing

9.1 Proliferation refers to the manufacture, acquisition, possession, developing, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. It includes technology, goods, software, services and expertise. Proliferation financing is the act of providing funds or financial services which are used, in whole or in part, to make proliferation possible (i.e., proliferation financing support of any part of the procurement process (this includes indirect coordination of the physical flow of goods). Financing can include financial transfers, mortgages, credit lines, insurance services, intermediary services, trust and corporate services and company formation.

9.2 The Proliferation Financing (Prohibition) Act, 2021 (PFPA) is the primary piece of legislation governing the criminalisation of proliferation of weapons of mass destruction and the provision of financing for such activities in the Virgin Islands. The implementation of the PFPA comes as a result of the recommendation made in the Virgin Islands' 2016 NRA to ensure compliance with FATF Recommendation 7. As such, the provisions within the PFPA seek to prevent the proliferation of WMD and their financing and are fashioned off FATF Recommendation 7 on targeted financial sanctions (TFS) related to proliferation.

9.3 The PFPA defines PF as the act of making available an asset, providing a financial service or conducting a financial transaction that facilitates:

- the manufacture, production, possession, acquisition, stockpiling, storage, development, transportation, sale, supply, transfer, export, trans-shipment or use of:
- nuclear, chemical or biological weapons; or
- materials related to nuclear, chemical, biological or radiological weapons that are restricted or prohibited.

9.4 Three elements (or stages) are frequently a feature of PF:

- Fundraising: a proliferator raises funds to finance PF;
- Disguising the funds: a proliferator transfers these funds into the international financial system for e.g. trade purposes. Proliferators rely on extensive networks of businesses (including front companies) and middlemen to obscure any connection on paper to sanctioned countries. Countries use opaque ownership structures for evading sanctions lists. Often proliferation financing involves companies in or near a sanctioned country and accounts under the control of a foreign national with sympathies to the sanctioned country. This, combined with the use of false documentation, allows proliferators to avoid detection; and
- Procurement of materials and technology: a proliferator or its agents uses those funds to pay for goods and services.

9.5 IBSPs must be able to distinguish between ML, TF and PF. The source of funds used to finance proliferation can be both legal and illegal. For example, international typologies show that in many cases the financing source is from a state or a person acting as an indirect agent of the state. While some risk indicators and control elements might overlap for ML, TF and PF, PF has its own unique risk indicators that financial institutions should implement: For example, PF red flags may include:

- Transactions involve foreign country of proliferation concern (i.e. Iran and North Korea) or country of diversion concern (e.g. China, Hong Kong, Singapore and Malaysia);
- Transactions include countries that are known to trade with North Korea (including Syria, Egypt, the United Arab Emirates, Yemen and Iran);
- Transaction involves financial institutions with known deficiencies in AML/CFT controls or located in weak export control and enforcement jurisdiction. For example, it is known that North Korea has used correspondent accounts held with Chinese banks to facilitate its international financial transfers;
- Customer activity does not match business profile or end-user information does not match end-user profile. A customer engages in a transaction that lacks business sense or strategy, or that is inconsistent with historical pattern of trade activity;
- Transaction concerns dual-use goods or military goods;

- Wire transfer or payment from or due to parties not identified on documentation or the transaction involves an unusual intermediary, or payment to be made to a beneficiary in a country other than the beneficiary's stated location; and
- Pattern of wire transfers or payment activity that shows unusual patterns or has no apparent purpose, or payment instructions are illogical or contain last minute changes.

9.6 IBSPs, should ensure that their systems and controls are properly developed to aid in identifying the proliferation financing risks and vulnerabilities to which they are exposed and also in the development of their systems and controls to prevent, detect and report proliferation financing. This is particularly important given that proliferation financing activities may be channeled through an IBSP towards the acquisition or refinement of nuclear materials by bad actors. This potential risk exposure to IBSPs can lead to catastrophic consequences for societies that could be the target of an attack using nuclear materials. The cascading consequences of failing to detect and prevent proliferation financing by a VI licensed IBSP can result in significant harm to international peace and security where such entities are found to have facilitated the proliferation of weapons of mass destruction. The fallout from this can bring harm to the Territory's reputation and its ability to continue operating as an international financial services center if found to be non-compliant with international standards related to PF. For the IBSP it can result in the imposition of significant penalties, loss of authorisation, and imposition of penalties for directors, senior officers and beneficial owners of the IBSP, as well as possible criminal charges being brought on the IBSP and its directors/senior officers. IBSPs must, therefore, fully implement the requirements of relevant proliferation financing laws in the VI as well have full regard and ensure their risk management processes account for the findings of the Virgin Islands Proliferation Financing Risk Assessment, 2022.

10. Targeted Financial Sanctions and Sanction Screening

10.1 At the point of onboarding a client, an IBSP is expected to ensure that sanctions screening is carried out and the results obtained in order to properly determine whether to take on a client. During the course of business with existing clients, it is essential for IBSPs to have effective systems in place that allow for immediate sanctions screening where new sanctions are imposed or existing sanctions are updated. Consequently, it is expected that IBSPs should be able to screen its client base within 24 hours of the imposition of newly designated sanctioned subjects, or updates to existing sanctions orders in order to identify any possible designated persons and take appropriate measures in keeping with the requirements of targeted financial sanctions orders, including freezing and reporting. IBSPs should also consider exposures that may exist with third party service providers and other intermediaries that may present heightened risks to sanctions compliance.

10.2 IBSPs must ensure that they have mechanisms in place to promptly act on new sanctions designations. Such mechanisms could include subscription directly to the UN or the UK Office of Financial Sanctions Implementation (OFSI) websites for the most up to date sanctions lists to ensure that customers, clients, or applicants for businesses are not designated persons. Additionally, IBSPs must have mechanisms in place to regularly keep up-to-date with changes to the BVI sanctions regime, as well as international sanctions that impact the BVI. Further information can be found at https://www.bvifsc.vg/about-sanctions-1.

10.3 Where an IBSP has detected a customer or assets of someone that has been the subject of a sanction, they are required to take freezing actions, prohibit transactions and report to BVI Competent Authorities (Governor's Office, and FIA as relevant) without delay. In addition, IBSPs should ensure that they review, are fully familiar with and implement the Virgin Islands Financial Sanctions Guidelines to ensure a thorough understanding of the systems and controls required to detect sanctioned subjects, as well as the actions required to ensure compliance with the sanctions regime in the BVI. An extract from these Guidelines, which sets out key definitions, is provided below at **Box 2**.

Box 2: Extracts from the Virgin Islands Financial Sanctions Guidelines[17]

Reporting Obligations

Financial sanctions obligations under the OICs require all relevant firms, natural and legal persons, entities and bodies to inform the Governor's Office as soon as practicable if they know or have reason to suspect a person is designated or has committed offences that do not 'facilitate compliance' with the regulations through which the VI implements targeted financial sanctions.

The requirement to comply with the reporting obligations applies to the relevant firm, relevant business, entity or profession that is:

- A body registered, incorporated or constituted under the laws of the VI or any part of the Territory and regulated by the FSC;
- A body registered, or constituted under the laws of the VI or any part of the Territory and supervised by the FIA; and
- any person onboard a ship or aircraft that is registered in the Territory.

How to Report

A Compliance Reporting Form ("CRF") must be completed when making a report to the Governor's Office. The CRF should be used when reporting suspected designated persons, any assets which have been frozen, and suspected breaches of financial sanctions and should be e-mailed to: Govofficesanctions.tortola@fcdo.gov.uk.

What Must a Relevant Firm/Business or Profession[18] Report?

If you are a relevant firm, business or profession you are required to report to the Governor's Office as soon as practicable:
(a) if you know or have a reasonable cause to suspect that a person is a designated person or has committed offences under financial sanctions legislation;
(b) the information, or other matter on which your knowledge or suspicion is based, if it came to you in the course of conducting business.

[17] IBSPs should refer to the VI Sanctions Guidelines for full details on their reporting obligations
[18] See definitions of "relevant firm", "relevant business" and "reporting entity" on pgs. 27 and 28 of the VI Sanctions Guidelines

Where you know or have reasonable cause to suspect that you are dealing with a designated person or entity and that person or entity is a customer of your firm or business, then you are required to submit a Compliance Reporting form to the GO, and in your reporting must include:

- information on which the knowledge or suspicion is based (including any potential or confirmed matches); and
- any information you hold about the person by which the person can be identified.

Where the person is a customer of a relevant firm or business, then the relevant firm or business must also state the nature and amount or quantity of any funds or economic resources held by it for the customer at the time when it first had the knowledge or suspicion

Other Reporting Obligations

In addition to reporting to the Governor's Office, a relevant firm, business, or reporting entity is obligated to report to the FIA any actions it has taken in respect of a suspected breach of sanctions by a designated person/entity (including any assets which have been frozen) or actions taken in respect of a de-listed person/entity, (including details of any assets which have been unfrozen). In this regard, relevant firms, businesses and reporting entities are required to maintain their requisite reporting obligations and/or to also submit Suspicious Activity/Transaction Reports (SARs/STRs) to the FIA. (Refer to "Compliance and Enforcement").

Pursuant to Part VII, Sections 60 and 61 of the CTA, relevant firms, relevant businesses, professionals and reporting entities are required to report to the FIA any suspicious activities /transactions relating to:

- Terrorist financing and terrorist acts;
- Property owned or controlled, directly or indirectly by a designated terrorist entity; and
- Property derived or generated from any property of the kind specified above.

Pursuant to Part IV of the PFPA, a person is required to report to the FIA if they hold an asset or assets suspected of being owned, controlled or held on behalf of, or at the direction of a designated person or entity.

For avoidance of doubt, all relevant entities and professionals are subject to the requirements under the AML/CFT regime, including the obligation to ensure that there are established internal control procedures and reporting mechanisms. In addition to the general reporting obligations to which relevant entities are subject, and where there is reasonable cause for suspicion, all relevant entities are required to report any suspected breaches in relation to targeted UN or UK financial sanctions to the Governor.

Save for information that comes to the attention of a professional legal adviser in privileged circumstances, failure to comply with the reporting obligations set out in the relevant legislation constitutes an offence which may result in criminal prosecution. Such reporting obligations are in addition to any other non-financial sanctions reporting obligations to which the relevant entity/institution may be subject (i.e. the filing of suspicious activity/transaction reports to the FIA, etc.).

11. Filing of Suspicious Activity/Transaction Reports

11.1 IBSPs must ensure that their compliance framework includes mechanisms, polices, procedures and internal controls to promptly report suspicious activities internally and report suspicious transactions to the FIA. IBSPs must ensure that any mechanism accounts for, amongst other things, attempted activity, transactions or customer relationships that the IBSP has refused. A suspicious activity will often be one that is inconsistent with a customer's known or typical business activities.

11.2 Accordingly, IBSPs are required to appoint a qualified individual as its Money Laundering Reporting Officer ("MLRO") to file SARs/STRs. IBSPs are guided to note that section 17(1) of the AMLTFCOP requires the MLRO to make a report to the FIA of every suspicious transaction or customer. Further, section 18 of the AMLTFCOP requires each employee to report a suspicion to the MLRO and where the MLRO determines that the suspicion is not warranted a record of that decision must be keep and be available for competent authorities and law enforcement agencies upon request. IBSPs should pay special attention to all guidance, documents, typologies and forms issued by the FIA related to SARs including the Guidance Notes on Suspicious Transaction Reports[19].

11.3 A suspicious report may also be triggered by the actions of an intermediary or other party with whom an IBSP engages in securities related business. Suspicious reports must be made in a form that ensures compliance with section 55 of the AMLTFCOP. Therefore, IBSPs are guided to adhere to requirements of reporting SARs and STRs as a means of minimising risk including operational and reputational risks. Once a SAR/STR has been filed with the FIA, IBSPs should take swift action to mitigate the risk of being abused by that customer or intermediary or other party for criminal purposes. This may mean reassessing the risk entailed in the business relationship and escalating the relationship to senior management.

Tipping Off

11.4 IBSPs should also be mindful that if it or an employee knows or suspects that an ML/TF/PF investigation is happening or about to take place, it is an offence to disclose information to anyone else which is likely to prejudice that investigation. Therefore, where the suspicion includes an intermediary or other party, the suspicion or the filing of an SAR/STR should not be disclosed, as it is an offence to leak information that could prejudice any investigation conducted. This extends beyond ML, TF, PF or other investigations to disclosures which would prejudice a confiscation investigation. Interfering with documents and other materials relevant to an investigation are also offences. IBSPs must therefore ensure that all staff are appropriately trained and understand their legal obligations in relation to tipping off.

Red Flag Indicators

11.5 The FATF Guidance for a Risk-Based Approach for the Securities Sector sets out an extensive list of suspicious activity indicators that are relevant for IBSPs. IBSPs should be mindful that emerging indicators may present changing or new ML, TF and PF risks. Extracts of some suspicious activity indicators have been provided in **Box 3** below. Further examples can be found in schedule 3 of the AMLTFCOP.

[19] https://fiabvi.vg/Analysis-Investigation/Documents-and-Forms

Some of the warning signs are as follows:

a) customers who are unknown to the securities investment business and verification of identity / incorporation proves difficult;
b) customers who wish to deal on a large scale but are completely unknown to the securities investment business;
c) customers who wish to invest or settle using cash;
d) customers who use a cheque that has been drawn on an account other than their own;
e) customers who change the settlement details at the last moment;
f) customers who insist on entering into financial commitments that appear to be considerably beyond their means;
g) customers who accept relatively uneconomic terms, when with a little effort they could have a much better deal;
h) customers who have no obvious reason for using the services of the Securities Investment Business (e.g.: customers with distant addresses who could find the same service nearer their home base; customers whose requirements are not in the normal pattern of the service provider's business which could be more easily serviced elsewhere);
i) customers who refuse to explain why they wish to make an investment that has no obvious purpose;
j) customers who are introduced by an overseas agent based in a country noted for drug trafficking or distribution or a customer introduced by an overseas branch, affiliate or other service provider based in in a country not assessed by the FSP as having a low degree of risk of ML/TF;
k) customers who transfer funds or shares to accounts in a in a country not assessed by the FSP as having a low degree of risk of ML/TF;
l) customers who indulge in much activity with little or no profit over a number of jurisdictions;
m) customers who carry out large numbers of transactions with the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction, particularly if the proceeds are also then credited to an account different from the original account;
n) customers who purchase low grade securities in an overseas jurisdiction, sell locally and then purchase high grade securities with the proceeds;
o) customers who constantly pay-in or deposit cash to cover requests for bankers' drafts, money transfers or other negotiable and readily marketable money instruments;
p) customers who wish to maintain a number of trustee or customers' accounts which do not appear consistent with the type of business, including transactions which involve nominee names;
q) any transaction involving an undisclosed party;
r) transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral;
s) significant variation in the pattern of investment without reasonable or acceptable explanation.

Documenting SARs/STRs

11.6 IBSPs' internal controls must detail how an employee should report a suspicious activity and to whom. An internal SAR log should be maintained and should indicate, amongst other things, the date the suspicious activity took place, the date the report was made, the circumstances surrounding the activity and the outcome of the investigation. This requirement to document the outcomes of an investigation must be maintained in all instances, including where a decision is taken not to file an SAR/STR based on there being no substantiation of ML, TF or PF. However, where a Reporting Officer has substantiated the suspicion of ML, TF or PF, they are responsible for filing an SAR/STR to the BVI Financial Investigation Agency.

11.7 IBSPs are to remain vigilant and review publications of typologies of risks in relation to conduct of investment business services or the provision of investment business products. IBSPs should also pay particular attention to their specific circumstances and customers to ensure that they are able to identify suspicious factors which may present themselves or be unique to the IBSP, its services, products or its client base.

12. Employee Screening

12.1 To safeguard against ML/TF/PF and other risks, measures must also be in place to assess the competence and probity of employees at the time of recruitment, and intermittently thereafter. IBSPs must, therefore, ensure that they carry out thorough screening of their employees in accordance with section 49 of the AMLTFCOP. This requirement is also supported by FATF Guidance[20]. These assessments of employees must include background checks as well as an assessment of integrity, skills, knowledge, and expertise to ably carry out their functions. Additional assessments and screening of employees must also be carried out where there is an anticipated change in their role or functions towards mitigating operational and compliance risks. This is of particular importance where the employee is responsible for the implementation of or monitoring of AML/CFT/CPF controls, which may occur directly in relation to the compliance function, or indirectly in relation to other functions.

12.2 IBSPs must also ensure that the screening of employees is proportionate to the ML/TF/PF risks to which that employee may be exposed to, regardless of the level of seniority of any employee. In addition, systems must be established to address potential conflicts of interest for staff with AML/CFT/CPF responsibilities. IBSPs must also be aware of their responsibility to report employee misconduct to the FSC and where relevant any other competent authority.

13. Powers of the FSC

13.1 The FSC's powers include the ability to inspect a regulated entity or any other entity that falls under the supervisory remit of the FSC, including IBSPs. Inspections may occur without notice and include a review of compliance against AML/CFT/CPF laws, as well as other regulatory requirements. Where an IBSP may be operating in or from within the VI but has not been licensed, the remit of the FSC extends to such entities in so far as it relates to the ability to take enforcement action for unauthorized business. The FSC's powers also include its ability to take enforcement action for non-compliance with financial services legislation, including AML/CFT/CPF legislation, against an IBSP, its directors, shareholders, and senior officers.

14. Information Exchange

14.1 Information exchange between IBSPs and other financial institutions, as well as regulatory and law enforcement authorities, is an important part of the VI's strategy for combating ML/TF/PF and should

[20] The FATF's Risk-Based Approach for the Securities Sector, issued in 2018 can be found at https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Rba-securities-sector.html

also form part of the IBSP's ongoing controls. Where authorities are armed with suspicion or evidence of a person's link or suspected link to ML, TF, or PF, they should be able to share that information with the IBSPs so that the latter can better engage its processes in dealing with such a person. Conversely, IBSPs should also be able to share general information about the type and nature of suspicious activities that may be linked to ML, TF or PF with other financial institutions and government agencies, including the regulator, subject to the requirements to ensure that there is no tipping off related to a filing of a SAR. This can only help to strengthen the IBSP sector and insulate it from abuse and misuse for ML, TF and PF purposes.

14.2 There are various types of information that can be shared between regulatory and law enforcement agencies and IBSPs. Such information may include:

- ML/TF/PF risk assessments;
- General feedback on suspicious transaction reports and other relevant reports;
- Typologies of how money launderers or terrorist financiers have misused IBSPs;
- Targeted unclassified intelligence which, subject to appropriate safeguards such as confidentiality agreements, may be shared with IBSPs, either collectively or individually; and
- Sanctions lists issued through the Governor's Office and published by the FSC and FIA, that include countries, persons or organisations whose assets or transactions should be frozen pursuant to targeted financial sanctions.

14.3 Domestic cooperation and information exchange between IBSPs and the FSC (as the supervisor of the IBSP sector), among law enforcement and intelligence agencies, and between the FIA and FSC, is extremely important in the effective monitoring and/or supervision of the IBSP sector.

14.4 Cross-border information sharing between authorities and their international counterparts is also vitally important given the multi-jurisdictional reach of many IBSPs. IBSPs must, therefore, ensure that they fully comply with CDD and recordkeeping requirements, segregation of customers' assets, as well as all other requirements of the AMLTFCOP and AML Regulations to ensure that the VI is able to meet its international obligations including those relating to correspondent relationships.

14.5 IBSPs, therefore, have an obligation to cooperate and to respond to requests for information in a timely and efficient manner. Requests to IBSPs will come with specific timelines for response, ranging from as short as 24 hours. IBSPs' systems and controls must be able to facilitate such immediate release of accurate and up to date information. Failure to do so would result in enforcement action being taken.

15. Overarching Requirement for Compliance

15.1 All IBSPs must remain vigilant in relation to evolving ML, TF and PF threats, as well as other threats that can negatively impact their operations. To mitigate against these threats and risks, IBSPs must be diligent in the application of AML/CFT/CPF measures. These measures must be holistic and integrate prudent governance and modern risk management strategies with a robust compliance framework. IBSPs must remain agile and embed systems to allow for continual improvement in the efficiency and effectiveness of AML/CFT/CPF compliance.

Appendix

All IBSPs that operate under the Securities and Investment Business Act, 2010 may be licensed to conduct business as defined by category of business. These categories have been extracted and provided below.

Categories of business for which an Investment Business Service Provider may be licensed.

Dealing as agent in the course of a profession or non-investment business

Dealing in investments as an agent if—

(a) the dealing is undertaken in the course of carrying on any business or profession which does not otherwise constitute investment business;

(b) the dealing may reasonably be regarded as a necessary part of other services provided in the course of that business or profession; and

(c) the person dealing as agent—

(i) does not receive or is not separately remunerated or rewarded in respect of his or her dealing as agent; and

(ii) does not hold himself or herself out generally as providing the service of dealing as agent.

Dealing in Investments

(a) Buying, selling, subscribing for or underwriting investments as an agent.

(b) Buying, selling, subscribing for or underwriting investments as principal where the person—

(i) holds himself or herself out as willing, as principal, to enter into transactions of that kind at prices determined by him or her generally and continuously rather than in respect of each particular transaction;

(ii) holds himself or herself out as engaging in the business of underwriting investments of the kind to which the transaction relates;

(iii) holds himself or herself out as engaging, as a market maker or dealer, in the business of buying investments of the kind to which the transaction relates with a view to selling them; or

(iv) regularly solicits members of the public for the purpose of inducing them, whether as principals or agents, to buy, sell, subscribe for or underwrite investments and the transaction is, or is to be entered into, as a result of the person having solicited members of the public in that manner.

For the purposes of this paragraph, one investment is of the same kind as another investment if they both fall within the same paragraph of Schedule 1.

Arranging Deals in Investments

Making arrangements with a view to—

(a) another person (whether as a principal or an agent) buying, selling, subscribing for or underwriting a particular investment, being arrangements which bring about, or would bring about, the transaction in question; or

(b) a person who participates in the arrangements buying, selling, subscribing for or underwriting investments.

Managing Investments

(a) Managing investments belonging to another person in circumstances involving the exercise of discretion (other than as manager of a mutual fund).

(b) Acting as manager of a mutual fund.

Providing Investment Advice

(a) Advising a person on investments (other than as the investment adviser of a mutual fund) where the advice—

(i) is given to the person in his or her capacity as an investor, or a potential investor, or in his or her capacity as agent for an investor or potential investor; and

(ii) concerns the merits of the investor, or a potential investor, doing any of the following (whether as principal or agent) —

(A) buying, selling, subscribing for or underwriting a particular investment; or

(B) exercising any right conferred by an investment to acquire, sell, subscribe for, underwrite or convert an investment.

(b) Acting as the investment adviser of a mutual fund.

Providing Custodial Services with Respect to Investments

(a) Acting as custodian or depository of assets belonging to another person, other than as custodian of a mutual fund or trustee of unit trust, where—

(i) those assets include investments falling within paragraphs 1 to 6 of Schedule 1; or

(ii) the custodial (or depositary) arrangements are such that those assets may consist of or include investments specified in subparagraph *(a)*(i) and the arrangements have at any time been held out as being arrangements under which investments would be safeguarded.

(b) Acting as custodian of a mutual fund.

(c) Acting as the trustee of a unit trust.

Providing Administration Services with Respect to Investments

(a) Administering or arranging for the administration of assets belonging to another person (other than as administrator of a mutual fund) where—

(i) those assets include investments falling within paragraphs 1 to 6 of Schedule 1; or

(ii) the administration arrangements are such that those assets may consist of or include investments and the arrangements have at any time been held out as being arrangements under which investments would be administered.

(b) Acting as administrator, registrar or transfer agent of a mutual fund.

Operating an Investment Exchange

Providing a facility, whether by electronic means or otherwise, for the orderly trading of investments or for the listing of investments for the purposes of trading, by members of the investment exchange.

Managing Investments

The management of investments by a supplier of goods or services where the securities are, or are to be, managed for the purposes of, or in connection with, the sale of goods or the supply of services by the supplier to a customer or a related sale or supply is deemed not to constitute managing investments for the purposes of paragraph 3 of Part A in the circumstances and to the extent specified.

Providing Investment Advice

The following activities are deemed not to constitute providing investment advice for the purposes of paragraph 4 of Part A in the circumstances and to the extent specified—

(1) **Newspapers, broadcasting and information services**

The giving of investment advice in—

(a) a newspaper, journal, magazine or other periodical publication;

(b) a television or sound broadcast; or

(c) any electronic information service,

if the principal purpose of the publication, broadcast or information service, taken as a whole and including any advertisements contained in it, is not to induce persons to buy, sell, subscribe for or underwrite a particular investment.

(2) **Providing investment advice in the course of a non-investment business**

The giving of investment advice in the course of a business that does not constitute investment business where the person does not receive any remuneration for the advice and the advice is not, or does not include—

(a) a recommendation to a person to buy, sell, subscribe for or underwrite a particular investment or to exercise or refrain from exercising rights conferred by a particular investment;

(b) advice on the suitability of a particular investment for the person to whom, or in relation to whom, the advice is given; or

(c) advice on the characteristics or performance of a particular investment.

(3) **Providing investment advice in the course of a profession**

The giving of legal or accounting advice with respect to an investment by a person in the course of carrying on business as a legal practitioner or an accountant.

(4) **Trustee providing investment advice**

The giving of investment advice by a person as trustee to—

(a) a co-trustee for the purposes of the trust; or

(b) a beneficiary under the trust concerning the beneficiary's interest under the trust,

if the person does not otherwise carry on, or hold itself out as carrying on, the business of providing investment advice or managing investments.

(5) **Director providing investment advice**

The giving of investment advice by a director of a company to another director of the company for the purposes of the company, provided that the director does not otherwise carry on, or hold itself out as carrying on, the business of providing investment advice or managing investments.

(6) **Sale of goods and services**

The giving of advice by a supplier to a customer for the purposes of or in connection with the sale of goods or supply of services, or a related sale or supply, or to a person with whom the customer proposes to enter into a transaction for the purposes of or in connection with such a sale or supply or related sale or supply.